UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,397	10/16/2003	Graeme John Proudler	B-5268 621375-8	1309

7590 09/05/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
MORAN, RANDAL D	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/688,397	PROUDLER, GRAEME JOHN	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *35-42,44 and 46-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *35-42,44,46-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34, 43, and 45 have been canceled per amendment filed 6/8/2007. Claims 36-42, 44, and 46-49 are pending in this application.

2. NPL Document TCPA PC Specific Implementation Specification, Version 1.00, pp. 1-70, (September 9, 2001) is unreadable and has not been considered. The remainder of the IDS filed on 10/16/2003 has been considered by the examiner. change

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 35-42, 44, 46-49** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Challener (US 2002/0059286)**.

3. Considering **Claims 35-49,** Challener discloses a secure key-handling unit arranged to store a storage root key that forms the root node of a tree- structured node hierarchy (abstract) the non-leaf nodes of which, other than the root node,

each comprise, in encrypted form, a key used to encrypt the or each of its child nodes ([0021]), and insecure storage for storing the hierarchy nodes other than the root node [0021] lines 6-8); a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key ([0021]).

Challener does not explicitly disclose the key-handling unit comprising: a memory for storing a current decryption-root key; a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

Ishiguro discloses a the key-handling unit comprising: a memory for storing a current decryption-root key (column 6- lines 6-10); current-decryption-root setting arrangement for storing in said memory (column 5- lines 20-29), in decrypted form (column 7- lines 57-66), the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key (column 5- lines 20-29 and 42-53, column 6- lines 30-34, column 7- lines 34-66), the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed (column 4- lines 60-67, column 5- lines 1-13, the "work key" may be changed relative to how much information the user is authorized to access).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Challener by the current decryption-root arrangement as taught by Ishiguro to provide a decoding apparatus in which encryption keys can be managed with ease (Ishiguro- column 2- lines 10-11).

4. Considering **Claim 36,** the combination of Challener and Ishiguro discloses the setting arrangement for changing the current root node is enabled to do so only upon a predetermined set of at least one condition being met (Challener- [0007], Ishiguro- column 7- lines 43-66).

5. Considering **Claim 37,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises the receipt by the key handling unit of an authorization value indicative of particular digital data (Ishiguro- column 7- lines 39-42).

6. Considering **Claim 38,** the combination of Challener and Ishiguro discloses authorization value is a digest of a protected process associated with the node that is intended to be the new selected non-leaf node (Challener- p.5 right column, lines 14-17, Ishiguro- column 4 lines 25-34).

7. Considering **Claim 39,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises that a protected process associated

with the node that is intended to be the new selected non-leaf node is about to be run by the computing platform (Challener- [0021], if you are attempting to migrate keys and access them, you are also intending to unlock the nodes and run the process, Ishiguro- column 5- lines 14-19, column 8- lines 1-5).

8. Considering **Claim 40,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises that any other currently-activated processes running on the apparatus are benign (Challener- Fig. 9).

9. Considering **Claim 41,** the combination of Challener and Ishiguro does not explicitly disclose at least one predetermined condition comprises that the key-handling apparatus is requested to change the current root node by a root of trust of the apparatus.

Official notice is taken that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Challener and Ishiguro by the root change request coming from a root of trust as is well known in the art for the benefit of having a set of unconditionally trusted functions that must work properly no matter what software is executing on the platform, in order to be immune to software attacks. Ideally, it should also be immune to physical attack, to avoid the need to trust an owner or user of a platform.

10. Considering **Claim 42,** the combination of Challener and Ishiguro discloses upon start up of the computing platform, the node at the head of the hierarchy forms said selected non-leaf node (Challener- Fig. 5- item 501, upon start-up, the storage root key is always considered the current root node, Ishiguro- column 3- lines 30-39).

11. Considering **Claim 44,** the combination of Challener and Ishiguro discloses the key-handling unit is arranged to always hold securely the node at the head of the hierarchy, in unencrypted form (Challener- [0021] lines 8-11, Ishiguro- column 7- lines 63-66).

12. Considering **Claim 46,** the combination of Challener and Ishiguro discloses the key-handling unit is arranged to indicate the current root node by signing a value associated with the node using an identity key associated with the key-handling unit (Challener- [0028], [0029], the non-migratable storage key is used to create a signature that would be used to identify it to the chip, Ishiguro- column 7- lines 39-46).

13. Considering **Claim 47,** the combination of Challener and Ishiguro discloses the key-handling unit is so arranged that only a particular type of key node (Challener [0021] lines 24-27, only the key set to be migrated can be used as the current root node) herein a dynamic key node, can be used as the current root node in addition to the node at the head of the hierarchy (Challener- Fig 5, the

storage root key can be used as the root as well as the migratable key (i.e. the dynamic root), Ishiguro- column 4- lines 60-67, column 5- lines 1-13).

14. Considering **Claim 48,** the combination of Challener AND iSHIGUROdiscloses the key-handling apparatus is arranged, upon receipt of a corresponding command, to generate a dynamic root node as a node of said key hierarchy (Challener- [0007]).

15. Considering **Claim 49**, the combination of Challener and Ishiguro disclose the setting arrangement is arranged to permit the selected non-leaf node to be changed to one associated with a protected process upon receipt by the key-handling unit of a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes, the key of the non-leaf node associated with said protected process being available for use in relation to the protected process upon becoming the decryption root key (Ishiguro- column 7- lines 39-66).

Response to Arguments

1. Applicant's arguments with respect to **claim 35** have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 2004/0153674 – designating a node in a hierarchy to be the root node and allowing access to all information descending from that root node.
- US 2003/0140277 – sub-root nodes allowing access to specified devices.
- US 2006/0159272 – enabling key blocks (EKB).
- US 2006/0004792 - Hierarchical storage architecture using node ID ranges.

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

8/23/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100